Exhibit 3

Security Rules and Procedures

Merchant Edition

22 February 2013

- A description of the Acquirer's chargeback controls in place to monitor the ECM's activities
- An evaluation of the practices that caused the ECM to exceed the ECP Standard
- An Acquirer action plan to reduce the ECM's CTR
- An electronic file that contains chargeback Transaction details for each chargeback received by the Acquirer for the ECM in the calendar month
- Any additional information as MasterCard may require from time to time

MasterCard will assess the Acquirer a reporting fee of USD 100 for each ECM report submitted.

8.3.2.2.2 Late ECM Report Submission Assessment

If MasterCard determines that a Merchant is an ECM and the Acquirer fails to submit a timely ECM report to MasterCard for that ECM, MasterCard may assess the Acquirer up to USD 500 per day for each of the first 15 days that the ECM report for that ECM is overdue and up to USD 1,000 per day thereafter until the delinquent ECM report is submitted.

8.3.3 Assessments

In addition to any applicable assessments for ECM reports or late report submissions, MasterCard may assess the Acquirer for Issuer reimbursement fees and violation assessments for excessive chargebacks arising from an ECM. MasterCard calculates the Issuer reimbursement fees and assessments as described in section 8.3.3.1 and they apply in each calendar month that the ECM exceeds a CTR of 150 basis points after the first trigger month. For the purposes of calculating Issuer reimbursement fees and assessments only (and not for the purpose of satisfying the reporting requirements contained herein), an Acquirer may offer an alternative CTR calculation that more accurately "maps back" or links the chargebacks to the relevant sales Transactions.

For the first 12 months of a Merchant's identification as an ECM, MasterCard will consider the Merchant's actual chargeback volume as a factor in its determination of Acquirer liability. During this period, MasterCard will assess the Acquirer the lesser of:

- The total of the Issuer reimbursement plus violation assessment amounts, calculated as described in section 8.3.3.1 for a given month, or
- The Merchant's chargeback dollar volume reported by the Acquirer for that month.

8.3.3.1 ECP Assessment Calculation

MasterCard determines an Acquirer's liability for the monthly Issuer reimbursement fees and assessments for each ECM as set forth below. MasterCard calculates the Issuer reimbursement fees in the following steps 1, 2, and 3, and calculates the violation assessment in step 4.

1. Calculate the CTR for each calendar month that the ECM exceeded a CTR of 150 basis points (which may also be expressed as 1.5% or 0.015).
2. From the total number of chargebacks in the above CTR calculation, subtract the number of chargebacks that account for the first 150 basis points of the CTR. (This amount is equivalent to 1.5 percent of the number of monthly sales Transactions used to calculate the CTR.) The result is the number of chargebacks above the threshold of 150 basis points.
3. Multiply the result from step 2 by USD 25. This is the Issuer reimbursement.
4. Adjust the result in step 3 to reflect the extent that the Acquirer has exceeded the 150 basis points threshold by multiplying the value in step 3 by the CTR (expressed as basis points). Divide this result by 100. This amount is the violation assessment.

Repeat steps 1–4 for each calendar month (other than the first trigger month) that the ECM exceeded a CTR of 150 basis points or 1.5 percent.

Example: The Acquirer for Merchant ABC acquired MasterCard sales Transactions and chargebacks over a six-month period as follows:

Month	January	February	March	April	May	June	July
Sales Transactions	95,665	95,460	95,561	95,867	95,255	95,889	95,758
Chargebacks	1,050	1,467	1,635	1,556	1,495	1,052	985
CTR in basis points	—	153	171	163	156	110	103

February and March are the trigger months, as these are two consecutive months where the CTR exceeded 150 basis points. At the end of July, Merchant ABC was no longer an ECM as its CTR was below 150 basis points for two consecutive months. MasterCard calculates assessments and Issuer reimbursements for each of the months March through July.

For example, the assessment for April (using March sales Transactions and April chargeback volumes) is calculated as follows:

- The CTR = April chargebacks/March sales Transactions = 1,556/95,561 = 0.01628 or 163 basis points (rounded)
- The number of chargebacks in excess of the 150 basis points is determined by subtracting 1.5 percent of the March sales Transactions from the number of April chargebacks. 1.5 percent of the March sales Transactions (95,561 x 0.015) is 1,433. 1,556 – 1,433 = 123 chargebacks
- The Issuer reimbursement for April is 123 x USD 25 = USD 3,075
- The violation assessment is (USD 3,075 x 163)/100 or 501,225/100 = USD 5,012.25

Using this methodology, the Issuer reimbursement fees and assessments for the Acquirer for Merchant ABC are as follows.

Month	Issuer Reimbursement	Assessment	Total
February (first trigger month)	0	0	0
March (second trigger month)	USD 5,075.00	USD 8,678.25	USD 13,753.25
April	USD 3,075.00	USD 5,012.25	USD 8,087.25
May	USD 1,425.00	USD 2,223.00	USD 3,648.00
June	0	0	0
July	0	0	0
Total	USD 9,575.00	USD 15,913.50	USD 25,488.50

Example: For the month of March, the Acquirer reported Merchant ABC chargeback volume of 1,635 chargebacks totaling USD 12,145. This amount is less than the calculated amount of the Issuer reimbursement plus violation assessment total of USD 13,753.25, as shown above for March. Therefore, MasterCard will assess the Acquirer the lesser chargeback volume amount rather than the greater calculated amount.

8.3.4 Issuer Reimbursement

MasterCard will remit Issuer reimbursement fees to Issuers through the MCBS. Actual reimbursements will vary depending on the extent and duration of the violation and the number of chargebacks processed by each Issuer, and will be paid out of the amounts collected for the Issuer reimbursement fees described in section 8.3.3.1 on a pro rata basis.

10.1 Account Data Protection Standards

PCI Security Standards are technical and operational requirements established by the Payment Card Industry Security Standards Council (PCI SSC) to protect account data. MasterCard requires that all Customers that store, process, or transmit Card, Cardholder, or Transaction data and all Customer agents that store, process, or transmit Card, Cardholder, or Transaction data on the Customer's behalf adhere to the most current Payment Card Industry PIN Transmission Security Program (PCI PTS) and *Payment Card Industry Data Security Standard* (PCI DSS). Customers and their agents also must ensure that:

- a terminal or other device at the Point of Interaction (POI) does not display, replicate, or store any Card-read data except Card account number, expiration date, service code, or Cardholder name; and
- before discarding any media containing Card, Cardholder, or Transaction data, including such data as account numbers, personal identification numbers (PINs), credit limits, and account balances, the Customer or its agent must render the data unreadable; and
- access to Card, Cardholder, or Transaction data stored in computers, terminals, and PCs is limited and controlled by establishing data protection procedures that include, but are not limited to, a password system for Computer Remote Terminal (CRT) access, control over dial-up lines, and any other means of access.

10.2 Account Data Compromise Events

Definitions

As used in this section 10.2, the following terms shall have the meaning set forth below:

Account Data Compromise Event or ADC Event	An occurrence that results, directly or indirectly, in the unauthorized access to or disclosure of MasterCard account data.
Agent	Any entity that stores, processes, or has access to MasterCard account data by virtue of its contractual or other relationship, direct or indirect, with a Customer. For the avoidance of doubt, Agents include, but are not limited to, Merchants, Third Party Processors (TPPs) and Data Storage Entities (DSEs) (regardless of whether the TPP or DSE is registered with MasterCard).
Customer	This term appears in the Definitions section at the front of the manual. For the avoidance of doubt, for purposes of this section 10.2, any entity that MasterCard licenses to issue a Card(s) and/or acquire a Transaction(s) shall be deemed a Customer.

Potential Account Data Compromise Event or Potential ADC Event	An occurrence that could result, directly or indirectly, in the unauthorized access to or disclosure of MasterCard account data.
Sensitive Card Authentication Data	This term has the meaning set forth in the *Payment Card Industry Data Security Standard*, and includes, by way of example and not limitation, the full contents of a Card's magnetic stripe or the equivalent on a chip, Card validation code 2 (CVC 2) data, and PIN or PIN block data.
Standards	This term appears in the Definitions section at the front of the manual.

10.2.1 Policy Concerning Account Data Compromise Events and Potential Account Data Compromise Events

MasterCard operates a payment solutions system for all of its Customers. Each Customer benefits from, and depends upon, the integrity of that system. ADC Events and Potential ADC Events threaten the integrity of the MasterCard system and undermine the confidence of Merchants, Customers, Cardholders, and the public at large in the security and viability of the system. Each Customer therefore acknowledges that MasterCard has a compelling interest in adopting, interpreting and enforcing its Standards to protect against and respond to ADC Events and Potential ADC Events.

Given the abundance and sophistication of criminals, ADC Events and Potential ADC Events are risks inherent in operating and participating in any system that utilizes payment Card account data for financial or non-financial Transactions. MasterCard Standards are designed to place responsibility for ADC Events and Potential ADC Events on the Customer that is in the best position to guard against and respond to such risk. That Customer is generally the Customer whose network, system or environment was compromised or was vulnerable to compromise or that has a direct or indirect relationship with an Agent whose network, system or environment was compromised or was vulnerable to compromise. In the view of MasterCard, that Customer is in the best position to safeguard its systems, to require and monitor the safeguarding of its Agents' systems and to insure against, and respond to, ADC Events and Potential ADC Events.

MasterCard requires that each Customer apply the utmost diligence and forthrightness in protecting against and responding to any ADC Event or Potential ADC Event. Each Customer acknowledges and agrees that MasterCard has both the right and need to obtain full disclosure (as determined by MasterCard) concerning the causes and effects of an ADC Event or Potential ADC Event as well as the authority to impose assessments, recover costs, and administer compensation, if appropriate, to Customers that have incurred costs, expenses, losses and/or other liabilities in connection with ADC Events and Potential ADC Events.

Except as otherwise expressly provided for in the Standards, MasterCard determinations with respect to the occurrence of and responsibility for ADC Events or Potential ADC Events are conclusive and are not subject to appeal or review within MasterCard.

Any Customer that is uncertain with respect to rights and obligations relating to or arising in connection with the Account Data Protection Standards and Programs set forth in this Chapter 10 should request advice from MasterCard Fraud Investigations.

Notwithstanding the generality of the foregoing, the relationship of network, system, and environment configurations with other networks, systems, and environments will often vary, and each ADC Event and Potential ADC Event tends to have its own particular set of circumstances. MasterCard has the sole authority to interpret and enforce the Standards, including those set forth in this chapter. Consistent with the foregoing and pursuant to the definitions set forth in section 10.2 above, MasterCard may determine, as a threshold matter, whether a given set of circumstances constitutes a single ADC Event or multiple ADC Events. In this regard, and by way of example, where a Customer or Merchant connects to, utilizes, accesses, or participates in a common network, system, or environment with one or more other Customers, Merchants, Service Providers, or third parties, a breach of the common network, system, or environment that results, directly or indirectly, in the compromise of local networks, systems, or environments connected thereto may be deemed to constitute a single ADC Event.

10.2.2 Responsibilities in Connection with ADC Events and Potential ADC Events

The Customer whose system or environment, or whose Agent's system or environment was compromised or vulnerable to compromise (at the time the ADC Event or Potential ADC Event occurred) is fully responsible for resolving all outstanding issues and liabilities to the satisfaction of MasterCard, notwithstanding any subsequent change in the Customer's relationship with any such Agent after the ADC Event or Potential ADC Event occurred. In the event of any dispute, MasterCard will determine the responsible Customer(s).

Should a Customer, in the judgment of MasterCard, fail to fully cooperate with the MasterCard investigation of an ADC Event or Potential ADC Event, MasterCard (i) may infer that information sought by MasterCard, but not obtained as a result of the failure to cooperate, would be unfavorable to that Customer and (ii) may act upon that adverse inference in the application of the Standards. By way of example and not limitation, a failure to cooperate can result from a failure to provide requested information; a failure to cooperate with MasterCard investigation guidelines, procedures, practices and the like; or a failure to ensure that MasterCard has reasonably unfettered access to the forensic examiner.

A Customer may not, by refusing to cooperate with the MasterCard investigation, avoid a determination that there was an ADC Event. Should a Customer fail without good cause to comply with its obligations under this section 10.2 or to respond fully and in a timely fashion to a request for information to which MasterCard is entitled under this section 10.2, MasterCard may draw an adverse inference that information to which MasterCard is entitled, but that was not timely obtained as a result of the Customer's noncompliance, would have supported or, where appropriate, confirmed a determination that there was an ADC Event.

Before drawing such an adverse inference, MasterCard will notify the Customer of its noncompliance and give the Customer an opportunity to show good cause, if any, for its noncompliance. The drawing of an adverse inference is not exclusive of other remedies that may be invoked for a Customer's noncompliance.

The following provisions set forth requirements and procedures to which each Customer and its Agent(s) must adhere upon becoming aware of an ADC Event or Potential ADC Event.

10.2.2.1 Time-Specific Procedures for ADC Events and Potential ADC Events

A Customer is deemed to be aware of an ADC Event or Potential ADC Event when the Customer or the Customer's Agent first becomes aware of an ADC Event or a Potential ADC Event. A Customer or its Agent is deemed to be aware of an ADC Event or Potential ADC Event under circumstances that include, but are not limited to, any of the following:

- the Customer or its Agent is informed, through any source, of the installation or existence of any malware in any of its systems or environments, or any system or environment of one of its Agents, no matter where such malware is located or how it was introduced;
- the Customer or its Agent receives notification from MasterCard or any other source that the Customer or its Agent(s) has experienced an ADC Event or a Potential ADC Event; or
- the Customer or its Agent discovers or, in the exercise of reasonable diligence, should have discovered a security breach or unauthorized penetration of its own system or environment or the system or environment of its Agent(s).

A Customer must notify MasterCard immediately when the Customer becomes aware of an ADC Event or Potential ADC Event in or affecting any system or environment of the Customer or its Agent. In addition, a Customer must, by contract, ensure that its Agent notifies MasterCard immediately when the Agent becomes aware of an ADC Event or Potential ADC Event in or affecting any system or environment of the Customer or the Agent.

When a Customer or its Agent becomes aware of an ADC Event or Potential ADC Event either in any of its own systems or environments or in the systems or environments of its Agent(s), the Customer must take (or cause the Agent to take) the following actions, unless otherwise directed in writing by MasterCard.

- Immediately commence a thorough investigation into the ADC Event or Potential ADC Event.
- Immediately, and no later than within twenty-four (24) hours, identify, contain, and mitigate the ADC Event or Potential ADC Event, secure MasterCard account data and preserve all information, in all media, concerning the ADC Event or Potential ADC Event, including:

  1. preserve and safeguard all potential evidence pertinent to a forensic examination of an ADC Event or Potential ADC Event;
  2. isolate compromised systems and media from the network;
  3. preserve all Intrusion Detection Systems, Intrusion Prevention System logs, all firewall, Web, database and events logs;
  4. document all incident response actions; and
  5. refrain from restarting or rebooting any compromised or potentially compromised system or taking equivalent or other action that would have the effect of eliminating or destroying information that could potentially provide evidence of an ADC Event or Potential ADC Event.

- Within twenty-four (24) hours, and on an ongoing basis thereafter, submit to MasterCard all known or suspected facts concerning the ADC Event or Potential ADC Event, including, by way of example and not limitation, known or suspected facts as to the cause and source of the ADC Event or Potential ADC Event.
- Within twenty-four (24) hours and continuing throughout the investigation and thereafter, provide to MasterCard, in the required format, all account numbers and expiration dates associated with MasterCard account data that were actually or potentially accessed or disclosed in connection with the ADC Event or Potential ADC Event and any additional information requested by MasterCard. As used herein, the obligation to obtain and provide account numbers to MasterCard applies to any MasterCard or Maestro account number in a bank identification number (BIN) range assigned by MasterCard. This obligation applies regardless of how or why such account numbers were received, processed or stored, including, by way of example and not limitation, in connection with or relating to a credit, debit (signature- or PIN-based) proprietary, or any other kind of payment Transaction, incentive or reward program.
- Within seventy-two (72) hours, engage the services of a PCI SSC Forensic Investigator (PFI) to conduct an independent forensic investigation to assess the cause, scope, magnitude, duration and effects of the ADC Event or Potential ADC Event. The PFI engaged to conduct the investigation must not have provided the last PCI compliance report concerning the system or environment to be examined. Prior to the commencement of such PFI's investigation, the Customer must notify MasterCard of the proposed scope

and nature of the investigation and obtain preliminary approval of such proposal by MasterCard or, if such preliminary approval is not obtained, of a modified proposal acceptable to MasterCard. MasterCard and the responsible Customer(s) may agree that a PFI's investigation of, investigation findings, and recommendations concerning fewer than all of the Merchants within the scope of the ADC Event or Potential ADC Event will be deemed to be representative of and used for purposes of the application of the Standards as the investigation findings and recommendations by the PFI with respect to all of the Merchants within the scope of the ADC Event or Potential ADC Event.

- Within two (2) business days from the date on which the PFI was engaged, identify to MasterCard the engaged PFI and confirm that such PFI has commenced its investigation.
- Within three (3) business days from the commencement of the forensic investigation, ensure that the PFI submits to MasterCard a preliminary forensic report detailing all investigative findings to date.
- Within twenty (20) business days from the commencement of the forensic investigation, provide to MasterCard a final forensic report detailing all findings, conclusions and recommendations of the PFI, continue to address any outstanding exposure, and implement all recommendations until the ADC Event or Potential ADC Event is resolved to the satisfaction of MasterCard. In connection with the independent forensic investigation and preparation of the final forensic report, no Customer may engage in or enter into any (or permit an Agent to engage in or enter into) any conduct, agreement or understanding that would impair the completeness, accuracy or objectivity of any aspect of the forensic investigation or final forensic report. The Customer shall not engage in any conduct (or permit an Agent to engage in any conduct) that could or would influence, or undermine the independence of, the PFI or undermine the reliability or integrity of the forensic investigation or final forensic report. By way of example, and not limitation, a Customer must not itself, or permit any of its Agents to, take any action or fail to take any action that would have the effect of:

  1. precluding, prohibiting or inhibiting the PFI from communicating directly with MasterCard;
  2. permitting a Customer or its Agent to substantively edit or otherwise alter the forensic report; or
  3. directing the PFI to withhold information from MasterCard.

Notwithstanding the foregoing, MasterCard may engage a PFI on behalf of the Customer in order to expedite the investigation. The Customer on whose behalf the PFI is so engaged will be responsible for all costs associated with the investigation.

10.2.2.2 Ongoing Procedures for ADC Events and Potential ADC Events

From the time that the Customer or its Agent becomes aware of an ADC Event or Potential ADC Event until the investigation is concluded to the satisfaction of MasterCard, the Customer must:

- Provide weekly written status reports containing current, accurate and updated information concerning the ADC Event or Potential ADC Event, the steps being taken to investigate and remediate same, and such other information as MasterCard may request.
- Preserve all files, data and other information pertinent to the ADC Event or Potential ADC Event, and refrain from taking any actions (e.g., rebooting) that could result in the alteration or loss of any such files, forensic data sources, including firewall and event log files, or other information.
- Respond fully and promptly, in the manner prescribed by MasterCard, to any questions or other requests (including follow-up requests) from MasterCard with regard to the ADC Event or Potential ADC Event and the steps being taken to investigate and remediate same.
- Authorize and require the PFI to respond fully, directly, and promptly to any written or oral questions or other requests from MasterCard, and to so respond in the manner prescribed by MasterCard, with regard to the ADC Event or Potential ADC Event, including the steps being taken to investigate and remediate same.
- Consent to, and cooperate with, any effort by MasterCard to engage and direct a PFI to perform an investigation and prepare a forensic report concerning the ADC Event or Potential ADC Event, in the event that the Customer fails to satisfy any of the foregoing responsibilities.
- Ensure that the compromised entity develops a remediation action plan, including implementation and milestone dates related to findings, corrective measures and recommendations identified by the PFI and set forth in the final forensic report.
- Monitor and validate that the compromised entity has fully implemented the remediation action plan, recommendations and corrective measures.

10.2.3 Forensic Report

The responsible Customer (or its Agent) must ensure that the PFI retain and safeguard all draft forensic report(s) pertaining to the ADC Event or Potential ADC Event and, upon request of MasterCard, immediately provide to MasterCard any such draft. The final forensic report required under section 10.2.2.1 must include the following, unless otherwise directed in writing by MasterCard:

- A statement of the scope of the forensic investigation, including sources of evidence and information used by the PFI.
- A network diagram, including all systems and network components within the scope of the forensic investigation. As part of this analysis, all system hardware and software versions, including Point-of-Sale (POS) applications and versions of applications, and hardware used by the compromised entity within the past twelve (12) months, must be identified.
- A payment Card Transaction flow depicting all Points of Interaction (POIs) associated with the transmission, processing and storage of MasterCard account data and network diagrams.
- A written analysis explaining the method(s) used to breach the subject entity's network or environment as well as method(s) used to access and exfiltrate MasterCard account data.
- A written analysis explaining how the security breach was contained and the steps (and relevant dates of the steps) taken to ensure that MasterCard account data are no longer at risk of compromise.
- An explanation of investigative methodology as well as identification of forensic data sources used to determine final report findings.
- A determination and characterization of MasterCard account data at risk of compromise, including the number of MasterCard accounts and at risk data elements (magnetic stripe data—Track 1 and Track 2, Cardholder name, primary account number [PAN], expiration date, CVC 2, PIN, and PIN block).
- The location and number of MasterCard accounts where restricted account data (magnetic stripe, Track 1 and Track 2, Cardholder name, PAN, expiration date, CVC 2, PIN, or PIN block), whether encrypted or unencrypyted, was or may have been stored by the entity that was the subject of the forensic investigation. This includes restricted MasterCard account data that was or may have been stored in unallocated disk space, backup media and malicious software output files.
- A time frame for Transactions involving MasterCard accounts determined to be at risk of compromise. If Transaction date/time is not able to be determined, file-creation timestamps must be supplied.
- A determination of whether a security breach that exposed payment card data to compromise occurred.
- On a requirement-by-requirement basis, a conclusion as to whether, at the time the ADC Event or Potential ADC Event occurred, each applicable PCI Security Standards Council requirement was complied with. For the avoidance of doubt, as of the date of the publication of these Standards, the PCI Security Standards include the PCI DSS, PIN Entry Device (PCI PED) Security Requirements, and *Payment Application Data Security Standard* (PA-DSS).

MasterCard may require the Customer to cause a PFI to conduct a PCI gap analysis and include the result of that analysis in the final forensic report.

The Customer must direct the PFI to submit a copy of the preliminary and final forensic reports to MasterCard via Secure Upload.

10.2.4 Alternative Standards Applicable to Certain Merchants

In the event of an ADC Event or Potential ADC Event (for purposes of this section 10.2.4, an "Event") for which the subject is a Level 2, Level 3, or Level 4 Merchant, in lieu of complying with the responsible Customer obligations set forth in section 10.2.2.1, the first bullet point of section 10.2.2.2, and section 10.2.3 of this Chapter 10, a responsible Customer may comply with the Standards set forth in this section 10.2.4 provided all of the following criteria are satisfied:

Criterion A — MasterCard determines that fewer than 7,500 accounts are at risk of unauthorized disclosure as a result of the Event; and

Criterion B — MasterCard determines that the Merchant has not been the subject of an ADC Event or Potential ADC Event for the thirty-six (36) consecutive months immediately preceding the date MasterCard determines likely to be the earliest possible date of the Event; and

Criterion C — The responsible Customer determines that the Merchant uses a computer-based acceptance system that is not used by another Merchant or Merchants and that is not operated by a Service Provider of the responsible Customer.

Should MasterCard determine that the subject of the Event is a Level 2, 3, or 4 Merchant and that Criteria A and B, above, are satisfied, MasterCard will provide notice to the responsible Customer via an e-mail message to the responsible Customer's Security Contact listed in the Member Information—MasterCard application then available on MasterCard Connect™.

Upon receipt of such notice, the responsible Customer may elect to cause a PCI SSC Forensic Investigator (PFI) to conduct an examination of the Merchant in accordance with section 10.2.2.1 of this Chapter 10. Alternatively, and provided the responsible Customer determines that Criterion C is satisfied, the responsible Customer itself may elect to investigate the Event in lieu of causing a PFI to conduct an examination of the Merchant.

If the responsible Customer itself elects to conduct the investigation, not later than sixty (60) days following the date of the notice by MasterCard described above, the responsible Customer must provide to MasterCard a written certification by an officer of the responsible Customer certifying that all of the following are true:

- That the responsible Customer elected to investigate the ADC Event or Potential ADC Event in lieu of causing a PFI to investigate the ADC Event or Potential ADC Event; and
- That the Merchant that is the subject of the ADC Event or Potential ADC Event does not use a computer-based acceptance system that is used by another Merchant or Merchants; and
- That the responsible Customer's investigation of the ADC Event or Potential ADC Event has been completed and that all security vulnerabilities have been eliminated; and
- That the Merchant has newly validated or revalidated compliance with the PCI DSS. Documentation confirming such validation or revalidation must be provided to MasterCard with the officer certification.

Except as specifically set forth in this section 10.2.4, all other MasterCard and Customer rights and obligations with respect to an ADC Event or Potential ADC Event shall continue with respect to any ADC Event or Potential ADC Event that a responsible Customer itself elects to investigate in accordance with this section 10.2.4. Further, and for the avoidance of doubt, MasterCard has a right at any time to require a responsible Customer to cause a PFI to conduct a forensic examination of a Merchant notwithstanding the provisions of this section 10.2.4.

10.2.5 MasterCard Determination of ADC Event or Potential ADC Event

MasterCard will evaluate the totality of known circumstances, including but not limited to the following, to determine whether or not an occurrence constitutes an ADC Event or Potential ADC Event:

- a Customer or its Agent acknowledges or confirms the occurrence of an ADC Event or Potential ADC Event;
- any PFI report; or
- any information determined by MasterCard to be sufficiently reliable at the time of receipt.

10.2.5.1 Assessments for PCI Violations in Connection with ADC Events

Based on the totality of known circumstances surrounding an ADC Event or Potential ADC Event, including the knowledge and intent of the responsible Customer, MasterCard (in addition to any assessments provided for elsewhere in the Standards) may assess a responsible Customer up to USD 100,000 for each violation of a requirement of the PCI Security Standards Council.

10.2.5.2 Potential Reduction of Financial Responsibility

Notwithstanding a MasterCard determination that an ADC Event occurred, MasterCard may consider any actions taken by the compromised entity to establish, implement, and maintain procedures and support best practices to safeguard MasterCard account data prior to, during and after the ADC Event or Potential ADC Event, in order to relieve, partially or fully, an otherwise responsible Customer of responsibility for any assessments, ADC operational reimbursement, ADC fraud recovery and/or investigative costs. In determining whether to relieve a responsible Customer of any or all financial responsibility, MasterCard may consider whether the Customer has complied with all of the following requirements:

- Substantiation to MasterCard from a PCI SSC-approved Qualified Security Assessor (QSA) of the compromised entity's compliance with the PCI DSS at the time of the ADC Event or Potential ADC Event.
- Reporting that certifies any Merchant(s) associated with the ADC Event or Potential ADC Event as compliant with the PCI DSS and all applicable MasterCard Site Data Protection (SDP) Program requirements at the time of the ADC Event or Potential ADC Event in accordance with section 10.3.3 of this manual. Such reporting must also affirm that all third party-provided payment applications used by the Merchant(s) associated with the ADC Event or Potential ADC Event are compliant with the *Payment Card Industry Payment Application Data Security Standard*, as applicable. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the *PCI PA-DSS Program Guide*, found at pcisecuritystandards.org.
- If the compromised entity is a Europe region Merchant, a PFI has validated that the Merchant was compliant with milestones one through four of the *PCI DSS Prioritized Approach* at the time of the ADC Event or Potential ADC Event.
- Registration of any TPP(s) or DSE(s) associated with the ADC Event through MasterCard Connect, in accordance with Rule 7.6 of the *MasterCard Rules*.
- Notification of an ADC Event or Potential ADC Event to and cooperation with MasterCard and, as appropriate, law enforcement authorities.
- Verification that the forensic investigation was initiated within seventy-two (72) hours of the ADC Event or Potential ADC Event and completed as soon as practical.
- Timely receipt by MasterCard of the unedited (by other than the forensic examiner) forensic examination findings.
- Evidence that the ADC Event or Potential ADC Event was not foreseeable or preventable by commercially reasonable means and that, on a continuing basis, best security practices were applied.

In connection with its evaluation of the Customer's or its Agent's actions, MasterCard will consider, and may draw adverse inferences from, evidence that a Customer or its Agent(s) deleted or altered data.

As soon as practicable, MasterCard will contact the Customer's Security Contact, Principal Contact, or Merchant Acquirer Contact as they are listed in the Member Information tool, notifying all impacted parties of the impending financial obligation or compensation, as applicable.

It is the sole responsibility of each Customer, not MasterCard, to include current and complete information in the Member Information tool.

10.2.5.3 ADC Operational Reimbursement and ADC Fraud Recovery

ADC operational reimbursement enables an Issuer to partially recover costs incurred in reissuing Cards and for enhanced monitoring of compromised and/or potentially compromised accounts associated with an ADC Event. ADC fraud recovery enables an Issuer to recover partial incremental magnetic-stripe (POS 90) and/or Hybrid POS Terminal unable to process (POS 80) counterfeit fraud losses associated with an ADC Event. MasterCard determines ADC operational reimbursement and ADC fraud recovery.

ADC operational reimbursement and ADC fraud recovery are available to an Issuer that is licensed to access MasterCard Alerts at the time of the ADC Event. MasterCard reserves the right to determine which ADC Events will be eligible for ADC operational reimbursement and/or ADC fraud recovery and to limit or "claw back" ADC operational reimbursement and/or ADC fraud recovery based on the amount collected from the responsible Customer, excluding assessments, or for the purpose of compromising any claim asserted that arises from or is related to an ADC Event.

With regard to any particular ADC Event, MasterCard has no obligation to disburse an amount in excess of the amount MasterCard actually and finally collects from the responsible Customer. In that regard, (i) any such amount actually and finally charged to a responsible Customer with respect to a particular ADC Event is determined by MasterCard following the full and final resolution of any claim asserted against MasterCard that arises from or is related to that ADC Event; and (ii) any funds disbursed by MasterCard to a Customer as ADC operational reimbursement and/or ADC fraud recovery is disbursed conditionally and subject to "claw back" until any claim and all claims asserted against MasterCard that arise from or are related to the ADC Event are fully and finally resolved.

MasterCard will charge the Issuer an administrative fee as established from time to time for administering the ADC operational reimbursement and ADC fraud recovery processes.

In the administration of the ADC operational reimbursement (OR) and ADC fraud recovery (FR) programs, MasterCard may determine the responsible Customer's financial responsibility with respect to an ADC Event. When determining financial responsibility, MasterCard may take into consideration the compromised entity's PCI level (as set forth in section 10.3.4), annual sales volume, and the factors set forth in section 10.2.5.2.

The annual sales volume is derived from the Merchant's clearing Transactions processed during the previous year via the Global Clearing Management System (GCMS). Transactions that are not processed by MasterCard will be included in the annual sales volume if such data is available. In the event that the Merchant's annual sales volume is not known, MasterCard will use the Merchant's existing sales volume to project the annual sales volume.

10.2.5.4 Operational Reimbursement (OR) Calculation

Subject to section 10.2.5.3, MasterCard generally calculates OR as follows:

1. Establish the total number of at-risk accounts per Issuer ICA number by type of Card, assuming one and one-half (1 1/2) Cards per account.
2. Subtract a fixed deductible (to be periodically published in a *Global Security Bulletin* or other MasterCard publication), to account for Card expirations, Card re-issuance cycles, accounts included in previous MasterCard Alerts and the re-issuance of accounts using the same PAN but a different expiration date.
3. Multiply the number of accounts by an amount fixed by MasterCard from time to time.
4. **United States region only**—For ADC Event investigation cases opened by MasterCard on or after 1 October 2013, subtract an additional 50 percent deductible from the product resulting from Step 3 if the compromised entity is a U.S. region Acquirer's Merchant located in the U.S. region and MasterCard determines that all of the following are true:

    a. At least 75 percent of the Merchant's annual total Transaction count originating from POS Terminals **and** the Transaction processing environment deemed by MasterCard to be within the scope of the ADC Event were processed through Dual Interface Hybrid POS Terminals at the time of the subject ADC Event.

    The Merchant's annual total Transaction count is determined based on the Merchant's clearing Transactions processed during the twelve (12) months prior to the date of publication of the MasterCard Alert, via the GCMS. Transactions that were not processed by MasterCard are included in the annual Transaction count if data is readily available to MasterCard. In the event that MasterCard is unable to readily determine the Merchant's annual total Transaction count, MasterCard may substitute any known Transaction count as a basis to project an annual total Transaction count; **and**

    b. The Merchant has not been identified by MasterCard as having experienced a different ADC Event during the twelve (12) months prior to the date of publication of the earliest MasterCard Alert for the subject ADC Event; **and**

    c. The Merchant was not storing Sensitive Card Authentication Data.

5. **United States region only**—Effective 1 October 2015, MasterCard will not assess for OR if the compromised entity is a U.S. region Acquirer's Merchant located in the U.S. region and MasterCard has determined that:

   a. At least 95 percent of the Merchant's annual total Transaction count originating from POS Terminals **and** the Transaction processing environment deemed by MasterCard to be within the scope of the ADC Event were processed through Dual Interface Hybrid POS Terminals at the time of the subject ADC Event.

      The Merchant's annual total Transaction count is determined based on the Merchant's clearing Transactions processed during the twelve (12) months prior to the date of publication of the MasterCard Alert, via the GCMS. Transactions that were not processed by MasterCard are included in the annual Transaction count if data is readily available to MasterCard. In the event that MasterCard is unable to readily determine the Merchant's annual total Transaction count, MasterCard may substitute any known Transaction count as a basis to project an annual total Transaction count; **and**

   b. The Merchant has not been identified by MasterCard as having experienced a different ADC Event during the twelve (12) months prior to the date of publication of the earliest MasterCard Alert for the subject ADC Event; **and**

   c. The Merchant was not storing Sensitive Card Authentication Data.

10.2.5.5 Fraud Recovery (FR) Calculation

MasterCard determines FR in the manner set forth in this section.

Subject to section 10.2.5.3, MasterCard determines an amount of incremental counterfeit fraud attributable to an ADC Event based on the fraud data reported to the System to Avoid Fraud Effectively (SAFE). As used in the immediately preceding sentence, the word "incremental counterfeit fraud" means counterfeit fraud incremental to the counterfeit fraud that MasterCard determines would have been expected to occur had the ADC Event not occurred.

NOTE

If the fraud type reported to SAFE for one or more fraud transactions is changed after MasterCard has calculated the ADC fraud recovery amount, MasterCard does not recalculate the ADC fraud recovery amount.

The calculation of FR uses an "at-risk time frame." The at-risk time frame may be known or unknown.

The at-risk time frame is "known" if MasterCard is able to determine a period of time during which accounts were placed at risk of use in fraudulent transactions due to or in connection with an ADC Event. In such case, the at-risk time frame for an account number commences as of the date that MasterCard determines that account became at risk, and ends, as the case may be, 30, 45, or 60 days after the date of publication of the earliest MasterCard Alert pertaining to that ADC Event disclosing that account number (see the *ADC User's Guide* for additional information).

The at-risk time frame is "unknown" if MasterCard is unable to determine a known at-risk time frame. In such event, an at-risk time frame for an account number commences twelve (12) months prior to the date of publication of the earliest MasterCard Alert for the ADC Event that discloses that account number, and ends, as the case may be, 30, 45, or 60 days after the date of publication of that MasterCard Alert (see the *ADC User's Guide* for additional information).

An account number disclosed in a MasterCard Alert in connection with a different ADC Event during the six (6) months prior to the earliest disclosure of that account number in a MasterCard Alert published in connection with the subject ADC Event is not eligible for ADC fraud recovery for the subject ADC Event. In addition, a standard deductible, published from time to time, is applied to compensate for chargeback recoveries on Transactions using at-risk account numbers and prior reissuance of at-risk account numbers with different expiration dates.

United States region only—MasterCard will:

1. For an ADC Event investigation case opened by MasterCard on or after 1 October 2013, apply an additional 50 percent deductible against the calculation of FR if the compromised entity is a U.S. region Acquirer's Merchant located in the U.S. region and MasterCard determines that all of the following are true:

   a. At least 75 percent of the Merchant's annual total U.S.-acquired Transaction count originating from POS Terminals **and** the Transaction processing environment deemed by MasterCard to be within the scope of the ADC Event were processed through Dual Interface Hybrid POS Terminals at the time of the subject ADC Event.

      The Merchant's annual total U.S.-acquired Transaction count is determined based on the Merchant's clearing Transactions processed during the twelve (12) months prior to the date of publication of the MasterCard Alert, via the GCMS. Transactions that were not processed by MasterCard are included in the annual U.S.-acquired Transaction count if the data is readily available to MasterCard. In the event that MasterCard is unable to readily determine the Merchant's annual total U.S.-acquired Transaction count, MasterCard may substitute any known U.S.-acquired Transaction count as a basis to project an annual total Transaction count; **and**

   b. The Merchant has not been identified by MasterCard as having experienced a different ADC Event during the twelve (12) months prior

to the date of publication of the earliest MasterCard Alert for the subject ADC Event; **and**

c. The Merchant was not storing Sensitive Card Authentication Data.

2. For an ADC Event investigation case opened by MasterCard on or after 1 October 2015, apply a 100 percent deductible against the calculation of FR if the compromised entity is a U.S. region Acquirer's Merchant located in the U.S. region and MasterCard determines that all of the following are true:

a. At least 95 percent of the Merchant's annual total U.S.-acquired Transaction count originating from POS Terminals **and** the Transaction processing environment deemed by MasterCard to be within the scope of the ADC Event were processed through Dual Interface Hybrid POS Terminals at the time of the subject ADC Event.

The Merchant's annual total U.S.-acquired Transaction count is determined based on the Merchant's clearing Transactions processed during the twelve (12) months prior to the date of publication of the MasterCard Alert, via the GCMS. Transactions that were not processed by MasterCard are included in the annual U.S.-acquired Transaction count if the data is readily available to MasterCard. In the event that MasterCard is unable to readily determine the Merchant's annual total U.S.-acquired Transaction count, MasterCard may substitute any known U.S.-acquired Transaction count as a basis to project an annual total Transaction count; **and**

b. The Merchant has not been identified by MasterCard as having experienced a different ADC Event during the twelve (12) months prior to the date of publication of the earliest MasterCard Alert for the subject ADC Event; **and**

c. The Merchant was not storing Sensitive Card Authentication Data.

10.2.5.6 Investigation and Other Costs

MasterCard may assess the responsible Customer for all investigation and other costs incurred by MasterCard in connection with an ADC Event and may assess a Customer for all investigative and other costs incurred by MasterCard in connection with a Potential ADC Event.

10.2.6 Assessments and/or Disqualification for Noncompliance

If the Customer fails to comply with the procedures set forth in this section 10.2, MasterCard may impose an assessment of up to USD 25,000 per day for each day the Customer is noncompliant and/or disqualify the Customer from participating as a recipient of ADC operational reimbursement and fraud recovery disbursements, whether such disbursements are made in connection with the subject ADC Event or any other ADC Event, from the date that MasterCard provides the Customer with written notice of such disqualification until MasterCard determines that the Customer has resolved all compliance issues under this section 10.2.

10.2.7 Final Financial Responsibility Determination

Upon completion of its investigation, if MasterCard determines that a Customer bears financial responsibility for an ADC Event or Potential ADC Event, MasterCard will notify the responsible Customer of such determination and, either contemporaneous with such notification or thereafter, specify the amount of the Customer's financial responsibility for the ADC Event or Potential ADC Event.

The responsible Customer has thirty (30) calendar days from the date of such notification of the amount of the Customer's financial responsibility to submit a written appeal to MasterCard, together with any documentation and/or other information that the Customer wishes MasterCard to consider in connection with the appeal. Only an appeal that both contends that the MasterCard financial responsibility determination was not in accordance with the Standards and specifies with particularity the basis for such contention will be considered.

If the appeal is timely and meets these criteria, MasterCard will consider the appeal and the documentation and/or other information submitted therewith in determining whether or not the MasterCard final financial responsibility determination was made in accordance with the Standards. An appeal that is not timely or does not meet these criteria will not be considered. The MasterCard decision with respect to an appeal is final and there are no additional internal appeal rights.

This section does not relieve a Customer of any responsibility set forth in sections 10.2.2 and 10.2.3, including the responsibility to submit to MasterCard on a continuing basis throughout the pendency of the MasterCard investigation the information required by those sections. If MasterCard determines that a Customer knew or should have known with reasonable diligence of documents or other information that the Customer was required to submit to MasterCard during the pendency of the MasterCard investigation in accordance with sections 10.2.2 or 10.2.3, but failed to do so, such documents or other information will not be considered by MasterCard in deciding the appeal.

10.3 MasterCard Site Data Protection (SDP) Program

The MasterCard Site Data Protection (SDP) Program is designed to encourage Customers, Merchants, Third Party Processors (TPPs), and Data Storage Entities (DSEs) to protect against account data compromises. SDP facilitates the identification and correction of vulnerabilities in security processes, procedures, and Web site configurations. For the purposes of the SDP Program, TPPs and DSEs are collectively referred to as "Service Providers" in this chapter.

Acquirers must implement the MasterCard SDP Program by ensuring that their Merchants and Service Providers are compliant with the *Payment Card Industry Data Security Standard (PCI DSS)* and that all applicable third party-provided payment applications used by their Merchants and Service Providers are compliant with the *Payment Card Industry Payment Application Data Security Standard* (PCI PA-DSS), in accordance with the implementation schedule defined in section 10.3.1 of this manual. Going forward, the *Payment Card Industry Data Security Standard* and the *Payment Card Industry Payment Application Data Security Standard* will be components of SDP; these documents set forth security Standards that MasterCard hopes will be adopted as industry standards across the payment brands.

A Customer that complies with the SDP Program requirements may qualify for a reduction, partial or total, of certain costs or assessments if the Customer, a Merchant, or a Service Provider is the source of an account data compromise.

MasterCard has sole discretion to interpret and enforce the SDP Program Standards.

10.3.1 Payment Card Industry Data Security Standards

The *Payment Card Industry Data Security Standard* and the *Payment Card Industry Payment Application Data Security Standard* establish data security requirements. Compliance with the *Payment Card Industry Data Security Standard* is required for all Issuers, Acquirers, Merchants, Service Providers, and any other person or entity a Customer permits, directly or indirectly, to store, transmit, or process account data. MasterCard requires validation of compliance only for those entities specified in the SDP Program implementation schedule in section 10.3.4. All Merchants and Service Providers that use third party-provided payment applications must only use payment applications that are compliant with the *Payment Card Industry Payment Application Data Security Standard*, as applicable. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the *PCI PA-DSS Program Guide*.

The *Payment Card Industry Data Security Standard*, the *Payment Card Industry Payment Application Data Security Standard*, the *PCI PA-DSS Program Guide*, and other PCI Security Standards manuals are available on the PCI Security Standards Council Web site at www.pcisecuritystandards.org.

10.3.2 Compliance Validation Tools

As defined in the implementation schedule in section 10.3.4, Merchants and Service Providers must validate their compliance with the *Payment Card Industry Data Security Standard* by using the following tools:

Onsite Reviews

The onsite review evaluates Merchant or Service Provider compliance with the *Payment Card Industry Data Security Standard*. Onsite reviews are an annual requirement for Level 1 Merchants and for Level 1 Service Providers. Merchants may use an internal auditor or independent assessor recognized by MasterCard as acceptable. Service Providers must use an acceptable third-party assessor as defined on the SDP Program Web site. Onsite reviews must be conducted in accordance with the *Payment Card Industry Security Audit Procedures* manual.

The *Payment Card Industry Self-assessment Questionnaire*

The *Payment Card Industry Self-assessment Questionnaire* is available at no charge on the PCI Security Standards Council Web site. To be compliant, each Level 2, 3, and 4 Merchant, and each Level 2 Service Provider must generate acceptable ratings on an annual basis.

Network Security Scan

The network security scan evaluates the security measures in place at a Web site. To fulfill the network scanning requirement, all Level 1 to 3 Merchants and all Service Providers as required by the implementation schedule must conduct scans on a quarterly basis using a vendor listed on the PCI SSC Web site. To be compliant, scanning must be conducted in accordance with the guidelines contained in the *Payment Card Industry DSS Security Scanning Procedures* manual.

10.3.3 Acquirer Compliance Requirements

To ensure compliance with the MasterCard SDP Program, an Acquirer must:

- For each Level 1, Level 2, and Level 3 Merchant, submit a quarterly status report via an e-mail message to sdp@mastercard.com using the form provided on the SDP Program Web site. This submission form must be completed in its entirety and may include information on:
  - The name and primary contact information of the Acquirer
  - The name of the Merchant
  - The Merchant identification number of the Merchant
  - The number of Transactions that the Acquirer processed for the Merchant during the previous 12-month period
  - The Merchant's level under the implementation schedule provided in section 10.3.4 of this manual
  - The Merchant's compliance status with its applicable compliance validation requirements

  - The Merchant's anticipated compliance validation date **or** the date on which the Merchant last validated its compliance (the "Merchant Validation Anniversary Date")

- Communicate the SDP Program requirements to each Level 1, Level 2, and Level 3 Merchant, and validate the Merchant's compliance with the *Payment Card Industry Data Security Standard* by reviewing its *Payment Card Industry Self-assessment Questionnaire* and the Reports on Compliance (ROC) that resulted from network security scans and onsite reviews of the Merchant, if applicable.
- Communicate the SDP Program requirements to each Level 1 and Level 2 Service Provider, and ensure that Merchants use only compliant Service Providers.

In submitting a quarterly SDP status report indicating that the Merchant has validated compliance within 12 months of the report submission date, the Acquirer certifies that:

1. The Merchant has, when appropriate, engaged and used the services of a data security firm(s) considered acceptable by MasterCard for onsite reviews, security scanning, or both.
2. Upon reviewing the Merchant's onsite review results, *Payment Card Industry Self-assessment Questionnaire*, or network scan reports, the Acquirer has determined that the Merchant is in compliance with the *Payment Card Industry Data Security Standard* requirements.
3. On an ongoing basis, the Acquirer will monitor the Merchant's compliance. If at any time the Acquirer finds the Merchant to be noncompliant, the Acquirer must notify the MasterCard SDP Department in writing at sdp@mastercard.com.

At its discretion and from time to time, MasterCard may also request the following information:

- Merchant principal data
- The name of any TPP or DSE that performs Transaction processing services for the Merchant's Transactions
- Whether the Merchant stores account data

When considering whether a Merchant stores account data, Acquirers carefully should survey each Merchant's data processing environment. Merchants that do not store account information in a database file still may accept payment Card information via a Web page and therefore store account data temporarily in memory files. Per the MasterCard data storage definition, any temporary or permanent retention of account data is considered to be storage. A Merchant that does not store account data never processes the data in any form, such as in the case of a Merchant that outsources its environment to a Web hosting company, or a Merchant that redirects customers to a payment page hosted by a third-party Service Provider.

10.3.4 Implementation Schedule

All onsite reviews, network security scans, and self-assessments must be conducted according to the guidelines in section 10.3.2. For purposes of the SDP Program, Service Providers in this section refer to TPPs and DSEs.

The Acquirer must ensure, with respect to each of its Merchants, that "transition" from one PCI level to another (for example, the Merchant transitions from Level 4 to Level 3 due to Transaction volume increases), that such Merchant achieves compliance with the requirements of the applicable PCI level as soon as practical, but in any event not later than one year after the date of the event that results in or causes the Merchant to transition from one PCI level to another.

All Level 1, 2, and 3 Merchants and all Service Providers that use any third party-provided payment applications must validate that each payment application used is listed on the PCI Security Standards Council Web site at www.pcisecuritystandards.org as compliant with the *Payment Card Industry Payment Application Data Security Standard*, as applicable. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the *PCI PA-DSS Program Guide*.

Level 1 Merchants

A Merchant that meets any one or more of the following criteria is deemed to be a Level 1 Merchant and must validate compliance with the *Payment Card Industry Data Security Standard*:

- Any Merchant that has suffered a hack or an attack that resulted in an account data compromise,
- Any Merchant having greater than six million total combined MasterCard and Maestro transactions annually,
- Any Merchant meeting the Level 1 criteria of Visa, and
- Any Merchant that MasterCard, in its sole discretion, determines should meet the Level 1 Merchant requirements to minimize risk to the system.

To validate compliance, each Level 1 Merchant must successfully complete:

- An annual onsite assessment conducted by a PCI Security Standards Council (SSC) approved Qualified Security Assessor (QSA) or internal auditor, and
- Quarterly network scans conducted by a PCI SSC Approved Scanning Vendor (ASV).

Level 1 Merchants that use internal auditors for compliance validation must ensure that primary internal auditor staff engaged in validating compliance with the *Payment Card Industry Data Security Standard* attend the PCI SSC-offered Internal Security Assessor (ISA) Program and pass the PCI SSC associated accreditation examination annually in order to continue to use internal auditors.

Level 2 Merchants

Unless deemed to be a Level 1 Merchant, the following are deemed to be a Level 2 Merchant and must validate compliance with the *Payment Card Industry Data Security Standard*:

- Any Merchant with greater than one million but less than or equal to six million total combined MasterCard and Maestro transactions annually, and
- Any Merchant meeting the Level 2 criteria of Visa.

To validate compliance, each Level 2 Merchant must successfully complete:

- An annual self-assessment, and
- Quarterly network scans conducted by a PCI SSC ASV.

Each Level 2 Merchant must ensure that staff engaged in self-assessing the Merchant's compliance with the *Payment Card Industry Data Security Standard* attend the PCI SSC-offered ISA Program and pass the associated PCI SSC accreditation examination annually in order to continue the option of self-assessment for compliance validation. Level 2 Merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA for an onsite assessment instead of performing a self-assessment.

Level 3 Merchants

Unless deemed to be a Level 1 or Level 2 Merchant, the following are deemed to be a Level 3 Merchant and must validate compliance with the *Payment Card Industry Data Security Standard*:

- Any Merchant with greater than 20,000 but less than or equal to one million total combined MasterCard and Maestro electronic commerce transactions annually, and
- Any Merchant meeting the Level 3 criteria of Visa.

To validate compliance, each Level 3 Merchant must successfully complete:

- An annual self-assessment, and
- Quarterly network scans conducted by a PCI SSC ASV.

Level 4 Merchants

Any Merchant not deemed to be a Level 1, Level 2, or Level 3 Merchant is deemed to be a Level 4 Merchant. Compliance with the *Payment Card Industry Data Security Standard* is required for a Level 4 Merchant, though validation of compliance (and all other MasterCard SDP Program Acquirer requirements set forth in section 10.3.3) is optional for a Level 4 Merchant. However, a validation of compliance is strongly recommended for Acquirers with respect to each Level 4 Merchant in order to reduce the risk of account data compromise and for an Acquirer potentially to gain a partial waiver of related assessments.

A Level 4 Merchant may validate compliance with the *Payment Card Industry Data Security Standard* by successfully completing:

- An annual self-assessment, and
- Quarterly network scans conducted by a PCI SSC ASV.

If a Level 4 Merchant has validated its compliance with the *Payment Card Industry Data Security Standard* and the *Payment Card Industry Payment Application Data Security Standard* as described in this section, the Acquirer may, at its discretion, fulfill the reporting requirements described in section 10.3.3.

Level 1 Service Providers

A Level 1 Service Provider is any TPP (regardless of volume) and any DSE that stores, transmits, or processes more than 300,000 total combined MasterCard and Maestro transactions annually.

Each Level 1 Service Provider must validate compliance with the *Payment Card Industry Data Security Standard* by successfully completing:

- An annual onsite assessment by a PCI SSC approved QSA, and
- Quarterly network scans conducted by a PCI SSC ASV.

Level 2 Service Providers

A Level 2 Service Provider is any DSE that is not deemed a Level 1 Service Provider and that stores, transmits, or processes 300,000 or less total combined MasterCard and Maestro transactions annually.

Each Level 2 Service Provider must validate compliance with the *Payment Card Industry Data Security Standard* by successfully completing:

- An annual self-assessment, and
- Quarterly network scans conducted by a PCI SSC ASV.

MasterCard has the right to audit Customer compliance with the SDP Program requirements. Noncompliance on or after the required implementation date may result in assessments described in Table 10.1.

Table 10.1—Assessments for Noncompliance with the SDP Program

Failure of the following to comply with the SDP Program mandate...	May result in an assessment of...
Classification	**Violations per calendar year**
Level 1 and Level 2 Merchants	Up to USD 25,000 for the first violation Up to USD 50,000 for the second violation Up to USD 100,000 for the third violation

Failure of the following to comply with the SDP Program mandate...	May result in an assessment of...
Classification	**Violations per calendar year**
	Up to USD 200,000 for the fourth violation
Level 3 Merchants	Up to USD 10,000 for the first violation Up to USD 20,000 for the second violation Up to USD 40,000 for the third violation Up to USD 80,000 for the fourth violation
Level 1 and Level 2 Service Providers	Up to USD 25,000 for the first violation Up to USD 50,000 for the second violation Up to USD 100,000 for the third violation Up to USD 200,000 for the fourth violation

Noncompliance also may result in Merchant termination, deregistration of a TPP or DSE as a Service Provider, or termination of the Acquirer as a Customer as provided in MasterCard Rule 1.6.2.

The Acquirer must provide compliance action plans and quarterly compliance status reports for each Level 1, Level 2, and Level 3 Merchant using the SDP Acquirer Submission and Compliance Status Form, available at http://www.mastercard.com/us/sdp/index.html or by contacting the MasterCard SDP Department at sdp@mastercard.com.

Acquirers must complete the form(s) in their entirety and submit the form(s) via e-mail message to sdp@mastercard.com on or before the last day of the quarter, as indicated below.

For this quarter...	Submit the form(s) no later than...
1 January to 31 March	31 March
1 April to 30 June	30 June
1 July to 30 September	30 September
1 October to 31 December	31 December

Late submission or failure to submit the required form(s) may result in an additional assessment to the Acquirer as described for Category A violations in MasterCard Rule 3.1.2.

10.3.4.1 MasterCard PCI DSS Risk-based Approach

A qualifying Level 1 or Level 2 Merchant located outside of the U.S. region may use the MasterCard PCI DSS Risk-based Approach, pursuant to which the Merchant:

- Validates compliance with the first four of the six total milestones set forth in the *PCI DSS Prioritized Approach*, as follows:
  - A Level 1 Merchant must validate compliance through an onsite assessment conducted by a PCI SSC-approved QSA, or by conducting an onsite assessment using internal resources that have been trained and certified through the PCI SSC-offered ISA Program.
  - A Level 2 Merchant must validate compliance using a Self-Assessment Questionnaire (SAQ) completed by internal resources that have been trained and certified through the PCI SSC-offered ISA Program. Alternatively, the Level 2 Merchant may validate PCI DSS compliance via an onsite assessment.
- Annually revalidates compliance with milestones one through four using an SAQ. The SAQ must be completed by internal staff trained and currently certified through the PCI SSC-offered ISA Program.

To qualify as compliant with the MasterCard PCI DSS Risk-based Approach, a Merchant must satisfy all of the following:

- The Merchant must certify that it is not storing Sensitive Card Authentication Data.
- On a continuous basis, the Merchant must keep fully segregated the "Card-not-present" Transaction environment from the "face-to-face" Transaction environment. A face-to-face Transaction requires the Card, the Cardholder, and the Merchant to all be present together at the time and place of the Transaction.
- For a Merchant located in the Europe region, at least 95 percent of the Merchant's annual total count of Card-present MasterCard and Maestro transactions must occur at Hybrid POS Terminals.
- For a Merchant located in the Asia/Pacific region, Canada region, Latin America and the Caribbean region, or South Asia/Middle East/Africa region, at least 75 percent of the Merchant's annual total count of Card-present MasterCard and Maestro transactions must occur at Hybrid POS Terminals.
- The Merchant must not have experienced an ADC Event within the last 12 months. At the discretion of MasterCard, this and other criteria may be waived if the Merchant validated full PCI DSS compliance at the time of the ADC Event or Potential ADC Event.
- The Merchant must establish and annually test an ADC Event incident response plan.

Information about the *PCI DSS Prioritized Approach* is available at:
www.pcisecuritystandards.org/education/prioritized.shtml

10.3.4.2 MasterCard PCI DSS Compliance Validation Exemption Program

A qualifying Level 1 or Level 2 Merchant may participate in the MasterCard PCI DSS Compliance Validation Exemption Program (the "Exemption Program"), which exempts the Merchant from the requirement to annually validate its compliance with the PCI DSS.

To qualify or remain qualified to participate in the Exemption Program, a duly authorized and empowered officer of the Merchant must certify to the Merchant's Acquirer in writing that the Merchant has satisfied all of the following:

1. The Merchant validated its compliance with the PCI DSS within the previous twelve (12) months or, alternatively, has submitted to its Acquirer, and the Acquirer has submitted to MasterCard, a defined remediation plan satisfactory to MasterCard designed to ensure that the Merchant achieves PCI DSS compliance based on a PCI DSS gap analysis;
2. The Merchant does not store Sensitive Card Authentication Data. The Acquirer must notify MasterCard through compliance validation reporting of the status of Merchant storage of Sensitive Card Authentication Data;
3. The Merchant has not been identified by MasterCard as having experienced an ADC Event during the prior twelve (12) months;
4. The Merchant has established and annually tests an ADC Event incident response plan in accordance with PCI DSS requirements; and
5. At least 75 percent of the Merchant's annual total acquired MasterCard and Maestro Transaction count is processed through Dual Interface Hybrid POS Terminals, as determined based on the Merchant's transactions processed during the previous twelve (12) months via the GCMS and/or Single Message System. Transactions that were not processed by MasterCard may be included in the annual acquired Transaction count if the data is readily available to MasterCard.

An Acquirer must retain all Merchant certifications of eligibility for the Exemption Program for a minimum of five (5) years. Upon request by MasterCard, the Acquirer must provide a Merchant's certification of eligibility for the Exemption Program and any documentation and/or other information applicable to such certification. An Acquirer is responsible for ensuring that each Exemption Program certification is truthful and accurate.

A Merchant that does not satisfy the Exemption Program's eligibility criteria, including any Merchant whose Transaction volume is primarily from e-commerce and Mail Order/Telephone Order (MO/TO) acceptance channels, must continue to validate its PCI DSS compliance in accordance with the MasterCard SDP implementation schedule.

All Merchants must maintain ongoing compliance with the PCI DSS regardless of whether annual compliance validation is a requirement.

10.3.4.3 Mandatory Compliance Requirements for Compromised Entities

Under the audit requirement set forth in section 10.2.2.1, the Acquirer must ensure that a detailed forensics evaluation is conducted.

At the conclusion of the forensics evaluation, MasterCard will provide a MasterCard Site Data Protection (SDP) Account Data Compromise Information Form for completion by the compromised entity itself, if the compromised entity is a TPP or DSE, or by its Acquirer, if the compromised entity is a Merchant. The form must be returned via e-mail to pci-adc@mastercard.com within 30 calendar days of its receipt, and must include:

- The names of the Qualified Security Assessor (QSA) and the Approved Scanning Vendor (ASV) that conducted the forensics evaluation, and
- The entity's current level of compliance with the *Payment Card Industry Data Security Standard*, and
- A gap analysis providing detailed steps required for the entity to achieve full compliance with the *Payment Card Industry Data Security Standard*.

As soon as practical, but no later than 60 calendar days from the conclusion of the forensics evaluation, the compromised entity or its Acquirer must provide evidence from a QSA and an ASV that the compromised entity has achieved full compliance with the *Payment Card Industry Data Security Standard*.

Such evidence (for example, a letter attesting to the entity's compliance, a compliance certificate, or a compliance status report) must be submitted to MasterCard via e-mail to pci-adc@mastercard.com.

Failure to comply with these requirements may result in SDP noncompliance assessments as described in section 10.3.4. Any Merchant or Level 1 or Level 2 Service Provider that has suffered a confirmed account data compromise will be automatically reclassified to become a Level 1 Merchant or a Level 1 Service Provider, respectively. All compliance validation requirements for such Level 1 entities will apply.

10.4 Connecting to MasterCard—Physical and Logical Security Requirements

Each Customer and any agent thereof must be able to demonstrate to the satisfaction of MasterCard the existence and use of meaningful physical and logical security controls for any communications processor or other device used to connect the Customer's processing systems to the MasterCard Worldwide Network (herein, "a MasterCard Network Device") and all associated components, including all hardware, software, systems, and documentation (herein collectively referred to as "Service Delivery Point Equipment") located on-site at the Customer or agent facility. Front-end communications processors include MasterCard interface processors (MIPs), network interface units (NIUs), and debit interface units (DIUs).

The controls must meet the minimum requirements described in this section, and preferably will include the recommended additional parameters.

10.4.1 Minimum Security Requirements

At a minimum, the Customer or its agent must put in place the following controls at each facility housing Service Delivery Point Equipment:

1. Each network segment connecting a MasterCard Network Device to the Customer's processing systems must be controlled tightly, as appropriate or necessary to prevent unauthorized access to or from other public or private network segments.
2. The connectivity provided by each such network segment must be dedicated wholly and restricted solely to the support of communications between MasterCard and the Customer's processing systems.
3. The Customer or its agent must replace each vendor-supplied or default password present on the Customer's processing systems, each MasterCard Network Device, and any device providing connectivity between them with a "strong password." A strong password contains at least eight characters, uses a combination of letters, numbers, symbols, punctuation, or all, and does not include a name or common word(s).
4. The Customer or its agent must conduct regular periodic reviews of all systems and devices that store MasterCard account information to ensure that access is strictly limited to appropriate Customer personnel on a "need to know" basis.
5. The Customer or its agent must notify MasterCard within 30 business days of any change in the personnel designated to administer the MasterCard Network Device. Refer to Appendix C of this manual for contact information.
6. The Customer or its agent must maintain and document appropriate audit procedures for each MasterCard Network Device. Audit reports must be maintained and accessible to the Customer for at least one year, including a minimum of 90 days in an easily retrieved electronic format.
7. The Customer must ensure that the software employed in any system or device used to provide connectivity to the MasterCard Worldwide Network is updated with all appropriate security patches, revisions and other updates as soon after a release as is practicable.
8. The physical location of the Service Delivery Point Equipment must be accessible only by authorized personnel of the Customer or its agent. Visitor access must be controlled by at least one of the following measures:
    a. Require each visitor to provide government-issued photo identification before entering the physical location; and/or
    b. Require each visitor to be escorted to the physical location by authorized personnel of the Customer or its agent.
9. If the physical location of the Service Delivery Point Equipment provides common access to other devices or equipment, then the MasterCard

Network Device must be stored in a cabinet that is locked both in front and the rear at all times. Keys to the cabinet must be stored in a secured location.

10. The Customer or its agent must have documented procedures for the removal of Service Delivery Point Equipment from the physical location.

10.4.2 Additional Recommended Security Requirements

Customers and their agents are strongly encouraged to put in place the following additional controls at each facility housing a MasterCard Network Device:

1. Placement of the MasterCard Network Device in a physical location that is enclosed by floor-to-ceiling walls.
2. Continual monitoring of the MasterCard Network Device by cameras or other type of electronic surveillance system. Video records should be maintained for a minimum of 90 days.

10.4.3 Ownership of Service Delivery Point Equipment

MasterCard is the sole and exclusive owner of all Service Delivery Point Equipment placed by MasterCard at the Service Delivery Point.

Effective as of date of placement, the Customer is granted a nonexclusive, non-assignable License to use the Service Delivery Point Equipment. The Customer may not take any action adverse to MasterCard with respect to its ownership of the Service Delivery Point Equipment.

The Customer at all times remains responsible for the safety and proper use of all Service Delivery Point Equipment placed at a location by request of the Customer, and must employ at that location the minimum security requirements set forth in this section 10.4. At its own expense, the Customer must promptly return all Service Delivery Point Equipment to MasterCard upon request of MasterCard and without such request, in the event of bankruptcy or insolvency.